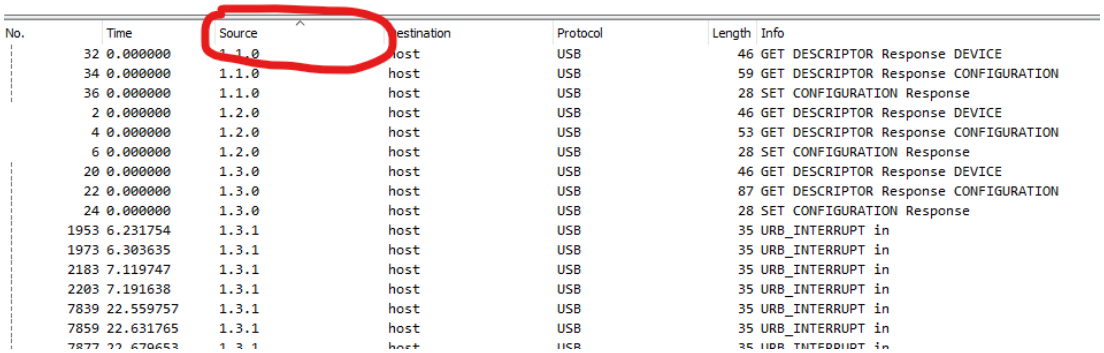
Hub (SOLUSI)

Solusi ini membutuhkan:

- Wireshark
- Python

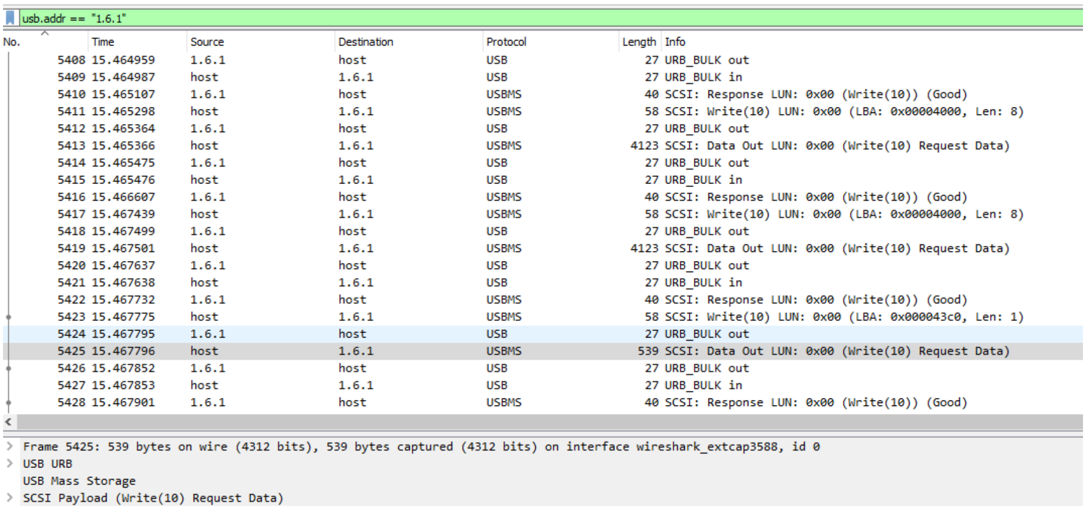
Langkah:

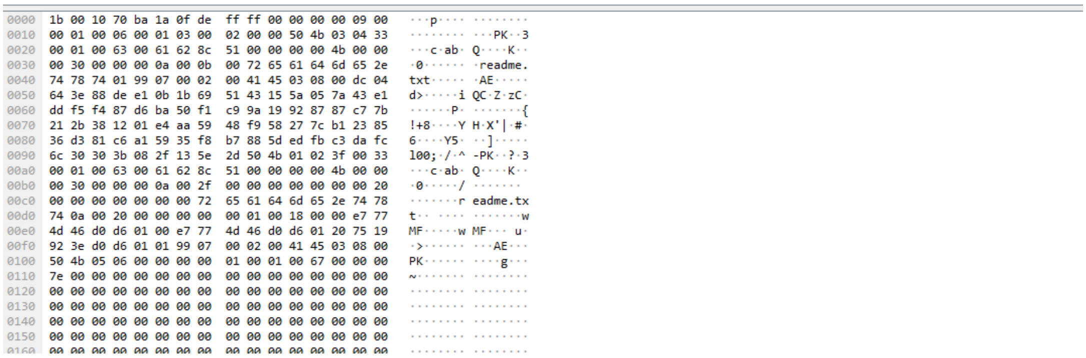
1. Membaca file .pcapng
   Hal yang dilakukan pertama adalah membaca file .pcapng tersebut. Dilihat sekilas, seluruh protokol yang berada dalam file .pcapng ini adalah USB. Terdapat 13 ribu entry packet yang lalu-lalang pada protokol USB, jadi perlu sedikit filtering terhadap data yang ditunjukkan. Cara yang paling mudah adalah melakukan sort terhadap sumber packet, lalu melihat obrolan pada masing-masing USB interface.



No.	Time	Source	Destination	Protocol	Length	Info
32	0.000000	1.1.0	host	USB	46	GET DESCRIPTOR Response DEVICE
34	0.000000	1.1.0	host	USB	59	GET DESCRIPTOR Response CONFIGURATION
36	0.000000	1.1.0	host	USB	28	SET CONFIGURATION Response
2	0.000000	1.2.0	host	USB	46	GET DESCRIPTOR Response DEVICE
4	0.000000	1.2.0	host	USB	53	GET DESCRIPTOR Response CONFIGURATION
6	0.000000	1.2.0	host	USB	28	SET CONFIGURATION Response
20	0.000000	1.3.0	host	USB	46	GET DESCRIPTOR Response DEVICE
22	0.000000	1.3.0	host	USB	87	GET DESCRIPTOR Response CONFIGURATION
24	0.000000	1.3.0	host	USB	28	SET CONFIGURATION Response
1953	6.231754	1.3.1	host	USB	35	URB_INTERRUPT in
1973	6.303635	1.3.1	host	USB	35	URB_INTERRUPT in
2183	7.119747	1.3.1	host	USB	35	URB_INTERRUPT in
2203	7.191638	1.3.1	host	USB	35	URB_INTERRUPT in
7839	22.559757	1.3.1	host	USB	35	URB_INTERRUPT in
7859	22.631765	1.3.1	host	USB	35	URB_INTERRUPT in

2. Mengekstrak hal yang menarik
   Setelah melakukan skimming terhadap PCAP yang telah disort, terdapat sebuah sumber dengan alamat 1.6.1 yang setelah dibaca DESCRIPTOR nya adalah sebuah USB drive. Apa yang biasanya dilakukan USB drive? Yak, transfer data. Dengan mengaplikasikan filter usb.addr == 1.6.1, kita bisa melihat apa yang dilakukan USB ini pada komputernya.

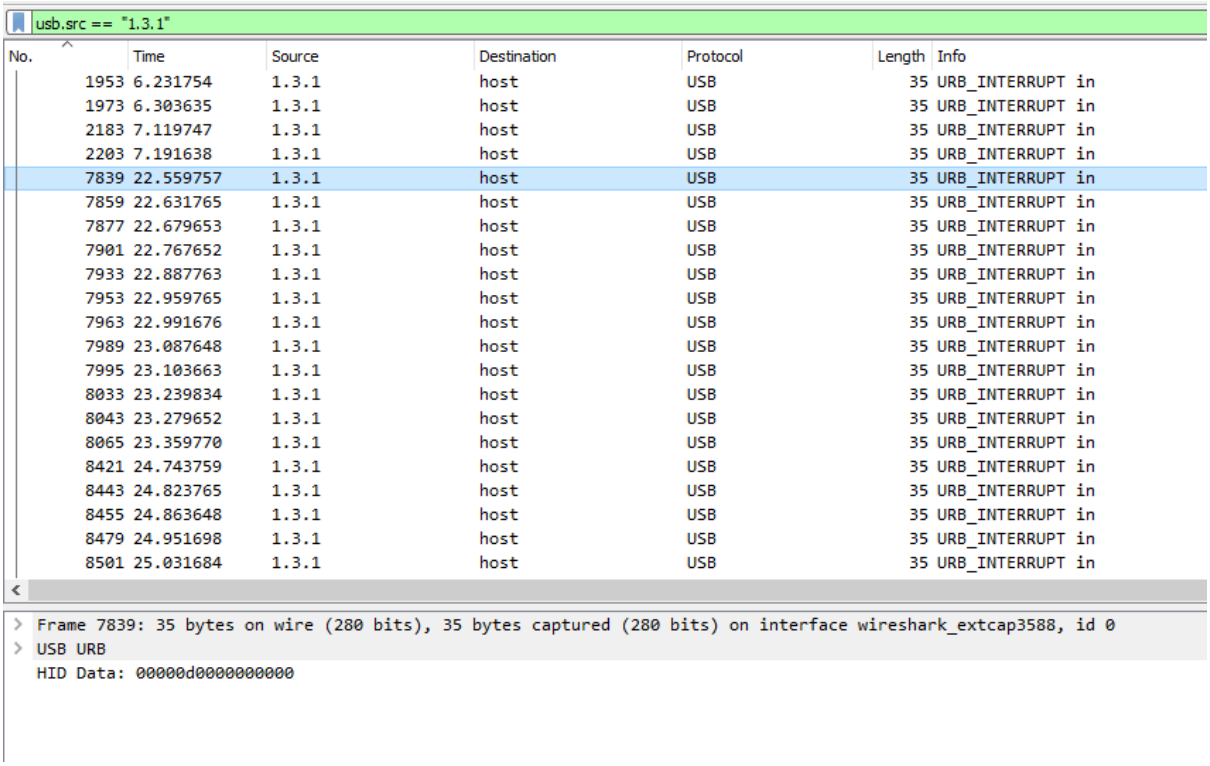




Dengan sedikit melihat-lihat, terdapat sebuah packet yang berisikan sebuah zipfile yang bisa diekstraksi. Ekstraksi yang paling jelas adalah dengan mengopi hex dari data tersebut kemudian ditaruh ke dalam sebuah file.

```python
ziphex =
"504b0304330001006300616 28c51000000004b000000300000000a000b00726561646d652e7478740199070
002004145030800dc04643e88dee10b1b695143155a057a43e1ddf5f487d6ba50f1c99a19928787c77b212b3
81201e4aa5948f958277cb1238536d381c6a15935f8b7885dedfbc3dafc6c30303b082f135e2d504b01023f0
033000100630061628c51000000004b000000300000000a002f000000000000002000000000000007265616
46d652e7478740a0020000000000000100180000e7774d46d0d60100e7774d46d0d601207519923ed0d601019
9070002004145030800504b0506000000000100010067000000 7e0000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000"

zipdata = bytes.fromhex(ziphex)

f = open("out.zip", "wb")

f.write(zipdata)

f.close()
```

3. Mengetahui bahwa file yang dikirimkan adalah zip yang dikunci dengan sebuah password
   Setelah dicoba dibuka, ternyata zip ini berpassword dan dienkripsi dengan AES-256. Dengan cara naif, mungkin beberapa akan mencoba untuk melakukan John the Ripper atau fcrackzip pada file ini. Namun karena passwordnya tidak berada di dalam dictionary manapun, mungkin peserta bisa terjebak pada rabbithole ini.
4. Mengekstrak dan menerjemahkan ketikan keyboard yang ditangkap pada file .pcapng tersebut
   Melihat hint yang diberikan, atau mungkin mendapat pencerahan dari langit, selain USB drive, terdapat juga USB device lain yang ditangkap pada file PCAP ini, salah satunya keyboard. Device lain yang terdapat pada file ini adalah mouse dan gamepad. Dengan menerapkan filter usb.src == "1.3.1", kita bisa melihat bahwa terdapat data yang dikirimkan oleh keyboard kepada host, yang menunjukkan bahwa seseorang sedang mengetik sesuatu pada saat USB di-capture.



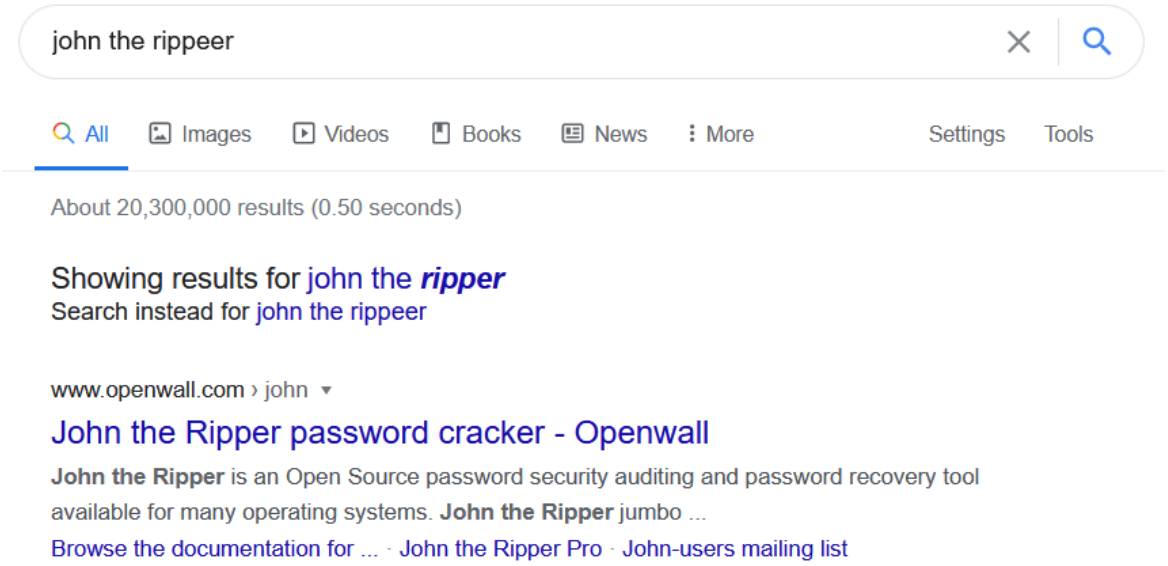
   Keyboard tidak mengirimkan data secara gamblang, namun berdasarkan standar USB keyboard. (https://www.usb.org/sites/default/files/documents/hut1_12v2.pdf) (Halaman 53)

Usage ID (Dec)	Usage ID (Hex)	Usage Name	Ref: Typical AT-101 Position	PC-AT	Mac	UNIX	Boot
0	00	Reserved (no event indicated)[9]	N/A	√	√	√	4/101/104
1	01	Keyboard ErrorRollOver[9]	N/A	√	√	√	4/101/104
2	02	Keyboard POSTFail[9]	N/A	√	√	√	4/101/104
3	03	Keyboard ErrorUndefined[9]	N/A	√	√	√	4/101/104
4	04	Keyboard a and A[4]	31	√	√	√	4/101/104
5	05	Keyboard b and B	50	√	√	√	4/101/104
6	06	Keyboard c and C[4]	48	√	√	√	4/101/104
7	07	Keyboard d and D	33	√	√	√	4/101/104
8	08	Keyboard e and E	19	√	√	√	4/101/104
9	09	Keyboard f and F	34	√	√	√	4/101/104
10	0A	Keyboard g and G	35	√	√	√	4/101/104
11	0B	Keyboard h and H	36	√	√	√	4/101/104
12	0C	Keyboard i and I	24	√	√	√	4/101/104
13	0D	Keyboard j and J	37	√	√	√	4/101/104
14	0E	Keyboard k and K	38	√	√	√	4/101/104
15	0F	Keyboard l and L	39	√	√	√	4/101/104
16	10	Keyboard m and M[4]	52	√	√	√	4/101/104
17	11	Keyboard n and N	51	√	√	√	4/101/104
18	12	Keyboard o and O[4]	25	√	√	√	4/101/104
19	13	Keyboard p and P[4]	26	√	√	√	4/101/104
20	14	Keyboard q and Q[4]	17	√	√	√	4/101/104

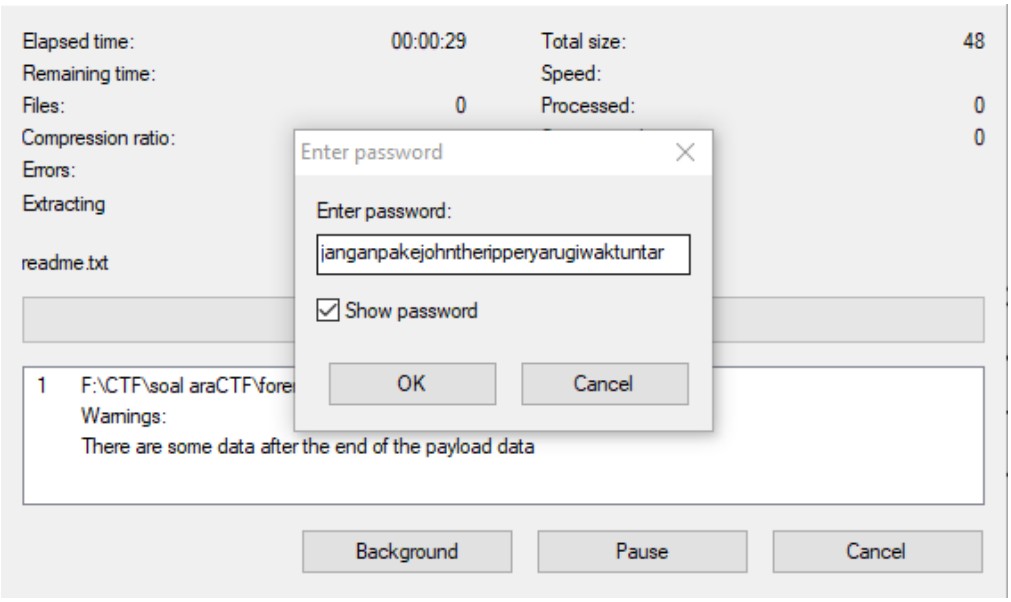
Kemudian data yang telah disaring dapat diexport menjadi JSON (File > Export Packet Dissection > As JSON...), kemudian diterjemahkan dengan script sebagai berikut:

```
import json

switcher = {'04': 'a', '05': 'b', '06': 'c', '07': 'd', '08': 'e', '09': 'f', '0A': 'g',
'0B': 'h', '0C': 'i', '0D': 'j', '0E': 'k', '0F': 'l', '10': 'm', '11': 'n', '12': 'o', '13':
'p', '14': 'q', '15': 'r', '16': 's', '17': 't', '18': 'u', '19': 'v', '1A': 'w', '1B': 'x',
'1C': 'y', '1D': 'x', '1E': '1', '1F': '2', '20': '3', '21': '4', '22': '5', '23': '6', '24':
'7', '25': '8', '26': '9', '27': '0', '2D': '-', '2E': '+', '2F': '[', '30': ']', '31': '"',
'33': ';', '34': "'", '35': '`', '36': ',', '37': '.', '38': '/'}

f = open("keyboard.json")

data = json.loads(f.read())

passwd = ""

for i in data:

        try:

                passwd += switcher[i["_source"]["layers"]["usbhid.data"][6:8].upper()]

        except:

                pass

print(passwd)
```

Output dari script tersebut adalah "janganpakejohntheripppeeryarugiwaktuntar". Karena sifat alamiah keyboard yang terkadang mengirimkan packet yang sama kedua kali ketika sebuah key ditekan terlalu lama, terkadang ada huruf yang muncul dobel pada packet. John the Ripper tidak dieja dengan dua huruf e, dapat digoogle ejaannya. Kata-kata yang seharusnya muncul pada keyboard adalah "janganpakejohntheripperyarugiwaktuntar".



5. Mengekstrak flag dengan password
   Dari kata-kata yang diekstrak tadi, "janganpakejohntheripperyarugiwaktuntar" adalah password dari zip yang kita ambil dari PCAP.



File readme.txt merupakan flagnya.
FLAG:
`ara2021{password_zip_alay_tapi_flag_jangan_alay}`